UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA,	)	
	)	
v.	)	**Crim. No. 08cr10318-NG**
	)	
STEPHEN WATT,	)	
Defendant.	)	

GERTNER, D.J.

SENTENCING MEMORANDUM
April 27, 2010

This case concerns what is reported to be the largest conspiracy to commit identity theft in American history. The defendant, Stephen Watt ("Watt"), played a unique role in the conspiracy, unique, that is, for run of the mill fraud crimes *before* the advent of the Internet. He adapted certain software that enabled the principals of the conspiracy to extract information from a number of companies, but he received no money for his work. He did it for the challenge, for the thrill of besting large institutions. But whatever the motive, however childish, morally irresponsible, not to mention legally culpable, it resulted in millions of victims and substantial losses.

To focus in sentencing on the man yields one result: He is a first offender with a supportive family and, by all accounts, a brilliant future. To focus on the crime yields another calculus. It was an extraordinary offense in scope and sophistication. This kind of dilemma is not unusual in a white collar case -- most are first offenders pulling off or trying to pull off a fraud -- but it is particularly stark here.

Watt, 25 years old, was charged in a one-count information with conspiracy, in violation of 18 U.S.C. § 371. He waived indictment and pled guilty pursuant to a plea agreement on

December 22, 2008. He was released on a $100,000 secured bond. He has been in substantial compliance with his conditions of release since that time.[1]

This Court held sentencing hearings over two days. At the initial hearing, the Court expressed concern that related cases[2] were in front of other judges at different stages of litigation, which could result in disparate treatment of similarly-situated offenders. No one judge could see

---

[1] With one exception: On February 12, 2009, pretrial services filed a petition for a summons to issue for Stephen Watt to appear for a show cause hearing with respect to his violation of his release conditions prohibiting the use of computers and access to the internet. The matter was resolved to the satisfaction of all concerned. He was otherwise in compliance with the terms of his release and has been since that date.

[2] Alberto Gonzalez: (08-cr-10223) pled guilty to a 19-count indictment (Judge Saris); also named in a 27-count indictment in the Eastern District of New York (E.D.N.Y. 08-cr-160) and a two-count indictment in the District of New Jersey (D. N.J. 09-cr-626); these cases have since been transferred to MA (09-cr-10262-Saris) (09-cr-10382-Woodlock). He had not been sentenced as of the date of Watt's sentencing. Gonzalez has since received a total of 240 months from Judge Saris in 08-cr-10223 and 216 months in 09-cr-10262 to run concurrent with the 240 months. Judge Woodlock sentenced him to 60 months for count 1 and 240 months and one day for count 2, also to run concurrent with the other sentences.

Christopher Scott: (08-10224) pled guilty to 4-count information; Judge Woodlock sentenced him to 84 months and 1 day.

Damon Toey: (08-10225) pled guilty to 4-count information; Judge Young sentenced him to 36 months.

Humza Zaman: (09-10054) pled guilty to 1-count information; Judge Wolf sentenced him to 46 months.

Jeremy Jethro: (09-10120) 1-count information; Judge Bowler sentenced him to three years' probation.

Maksym Yastremskiy: 27-count indictment, case pending in E.D.N.Y (EDNY 08-00160).

Aleksandr Suvorov: 27-count indictment, case pending in E.D.N.Y. (EDNY 08-00160).

Jonathan Williams: pled guilty to 8-count indictment in E.D.Pa. (EDPa 06-00170) and sentenced to 36 months.

It should be noted that the reason defendants who are part of the same conspiracy have been indicted before different judges is that there is no related case rule in criminal cases in the District of Massachusetts, as there is for civil cases. See Local Rule 40.1(G)(3) ("The clerk shall assign related [civil] cases to the same judge without regard to the number of other cases in that category previously assigned to that judge."); see also Amgen, Inc. v. F. Hoffmann-La Roche, Ltd., 480 F. Supp. 2d 462, 470-71 (D. Mass. 2007); Atl. Research Mktg. Sys. v. G.G.&G., L.L.C., 167 F. Supp. 2d 458, 460-461 (D. Mass. 2001). In order to compensate, the government represented that it intended to provide Probation and the Court with a statement of facts to reflect the status of all of the defendants who were charged as of the time Watt pled.

the entire picture. And without a global view, the Court could not comply with 18 U.S.C. § 3553(a)(6)'s direction, calling for "avoid[ing] unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct." When counsel at the first hearing also indicated that Watt made no money from his participation in the offense, the Court had new concerns -- what motivated him to participate, what brand of sociopathy, if any, did he suffer from -- and requested additional information about Watt.[3]

The parties could not have been further apart on sentencing. Defense counsel urged probation for a sentence of six months or less. The government pressed for the maximum sentence of five years. The Guidelines were of no help; if not for the statutory maximum, the Guidelines for an offense level 43 and criminal history *I* would have called for a sentence of life imprisonment.

I rejected the defendant's proposal as being unduly lenient. Substantial punishment was plainly called for because of what Watt did and why, as I describe below. But at the same time, I rejected the government's recommendation as too severe for a first offender under the circumstances. Accordingly, I sentenced Watt to 24 months of custody, three years of supervised release, and a substantial order of restitution, amounting to $171.5 million.

I. OFFENSE

From 2004 to 2007, Albert Gonzalez ("Gonzalez") and his associates stole over 40 million credit and debit card numbers from major retailers, including TJX companies, DSW, and BJ's Wholesale Club. The group tapped into the corporations' networks and lifted financial data using

[3] At the initial hearing, counsel for Watt, apparently trying to paint him in a better light, indicated that Watt did not know that helping someone steal is the same thing as stealing. The distinction was absurd. Transcript of June 8, 2009, p. 34.

sophisticated computer programs. Gonzalez then sold millions of these numbers overseas to third parties. Losses total $171.5 million for TJX,[4] between $6.5 and $9.5 million for DSW, and between $11 and $13 million for BJ's. According to the presentence report -- and uncontested -- the victims also include the thousands of banks who have had to cover the losses and the millions of individuals whose financial information was stolen. PSR ¶¶ 2, 5

A. The Gonzalez - Scott Conspiracy

From 2003 to 2006, Gonzalez and Christopher Scott ("Scott") hacked into computer networks for bizrate.com, panduck.com, fortunecity.com, and Florida International University. The two then hacked into BJ's through wireless access points located near the actual retail stores. Gonzalez stole and subsequently sold off 300,000 to 400,000 credit card numbers that Scott helped him obtain from BJ's. PSR ¶ 10.[5]

Scott then hacked into Office Max's system, captured debit card information, and gave this information to Gonzalez. PSR ¶ 12. Gonzalez sold some of these to co-conspirator Maksym Yastremskiy, and "cash[ed] out" others at ATMs through co-conspirator Jonathan Williams. PSR ¶ 13.

During the same period, Gonzalez was collaborating with Damon Patrick Toey ("Toey") to "cash out" payment card numbers and selling "dumps" of them. ("Dumps" are stolen track 2

[4] TJX has set aside an additional approximately $42.2 million to pay for its losses. PSR ¶ 5.

[5] According to the presentence report, Gonzalez had been arrested in July 2003 and had agreed to cooperate with the Secret Service in exchange for the dismissal of charges. PSR ¶ 6. Gonzalez cooperation obviously did not stop him from participating in the instant offense.

data, the data encoded on the magnetic strips on the backs of credit cards read by ATM machines and credit card readers.)[6] PSR ¶ 7 & n. 2.

[6] "After the BJ's intrusion, Jonathan James ("James") became involved in the hacking and downloading, while Gonzalez concentrated on selling the card data and handling the proceeds." PSR ¶ 11. James "committed suicide during the course of the investigation." PSR n. 3.

B. Watt's Role - TJX incursion

Beginning in the summer of 2005, Scott and Gonzalez hacked into TJX Companies, assisted by James. But their work was substantially improved when they used a wireless access point, together with a VPN (virtual private network), a program that allowed Gonzalez to access the TJX system without being in close physical proximity to a retail store. PSR ¶ 16.

Gonzalez used a "sniffer program" that allowed him to seek out the data he wanted, a program that Watt had adapted. PSR ¶¶ 16-16a. Sniffer programs are used both legally and illegally to monitor traffic in a computer network. They represent a class of applications that captures any type of data that travels across a communications network. PSR ¶ 16.

Instant message chat sessions between Watt and Gonzalez from February 24, 2005, until April 10, 2006, the year immediately preceding Watt's role in supplying the sniffer program, are significant to understand Watt's role and motivation. While it is difficult to evaluate whether these sessions reflect Watt's bravado and his stunning immaturity or what one psychologist calls the "online disinhibition effect,"[7] they do make clear that he understood that he was remotely

---

[7] John Suler, in a book entitled "The Psychology of Cyberspace," writes of the "online disinhibition effect."

> It's well known that people say and do things in cyberspace that they wouldn't ordinarily say or do in the face-to-face world. They loosen up, feel more uninhibited, express themselves more openly. Researchers call this the "disinhibition effect." It's a double-edged sword. Sometimes people share very personal things about themselves. They reveal secret emotions, fears, wishes. Or they show unusual acts of kindness and generosity. We may call this *benign disinhibition*.
>
> On the other hand, the disinhibition effect may not be so benign. Out spills rude language and harsh criticisms, anger, hatred, even threats. Or people explore the dark underworld of the internet, places of pornography and violence, places they would never visit in the real world. We might call this *toxic disinhibition*.

compromising software vulnerabilities on network systems, as well as utilizing stolen account credentials. And he plainly knew that Gonzalez was selling payment card numbers and making a substantial profit. At the same time, there is no persuasive evidence that Watt had access to the information being stolen, or participated in selling it. Indeed, as noted above, Watt received no money for his efforts.[8]

C. Gonzalez-Scott-Toey

The Gonzalez conspiracy not only predated Watt's participation, it also postdated it, operating between 2004 and 2007. In the fall of 2007, for example, Toey helped Gonzalez break into Target's computer system, using a high powered wireless antenna. PSR ¶ 17. He also assisted Gonzalez in breaking into Forever 21's system, now using a web-based attack. PSR ¶ 19. This approach involved gaining access to the companies' databases using vulnerabilities in its programming. PSR ¶ 18-19. Toey also set up computer servers for Gonzalez in Latvia and the

---

John Suler, The Online Disinhibition Effect, Psychology Of Cyberspace (June 2003), available at http://www.rider.edu/~suler/psycyber/disinhibit.html. (The Psychology of Cyberspace is a comprehensive, online book that is available at http://www.rider.edu/~suler/psycyber/psycyber.html and, using its title, through common search engines.)

He identifies many causes of the "disinhibition," including the practical anonymity of the internet, the physical invisibility of participants, and the sense that online activity is, effectively, a game. Then, quoting another scholar, Emily Finch, described as an author and criminal lawyer, he notes "that some people see their online life as a kind of game with rules and norms that don't apply to everyday living. . . . Why should they be held responsible for what happens in that make-believe play world that has nothing to do with reality? After all, it isn't that different than blasting away at your pals in a shoot-em up video game . . . or so some people might think, perhaps unconsciously." Id. This surely does not excuse Watt's activities, but it may explain some of his banter.

[8] The government contended that Watt participated in Gonzalez's money laundering, a fact contested by the defense, which cannot be resolved on this record, even by a fair preponderance of the evidence. Transcript of June 8, 2009, p. 22. The government also maintains that Watt participated in other technical aspects of the conspiracy, beyond adapting the "sniffer" program. It claims that he prepared a "Luhn checker" which was a mathematical algorithm that sorts numbers enabling some verification of credit card and debit card numbers. Id. at 42. Likewise, the government maintained that Watt wrote the code for a "track parser" which takes large blocks of information and divides it up into the credit card number and the various other information that is on the magnetic strip of a credit card. Defendant agrees that he prepared a Luhn checker but not the "track parser." Id.

Ukraine on which millions of payment numbers were stored. PSR ¶ 20. Scott used a server in California for TJX data. PSR ¶ 16.

Watt's "sniffer program" was on the Latvian server, but that file was independent from the locations where stolen credit cards where stored. PSR ¶ 20. There is no indication that Watt had access to the portions of the server on which data was stored. Cf. Transcript, December 22, 2009, p. 26, 47; PSR ¶ 20. In addition, during the execution of the search warrant at Watt's apartment, the IP address for the server on which TJX data was stored "was written on a piece of paper found in the closet where Watt's computer was set up." PSR ¶ 16a. But again, I cannot say by a fair preponderance of the evidence that Watt ever accessed the data on that server.

D. Watt's Employment

While Watt spent time online with Gonzalez, he also had full time employment. He first did demolition work for a contractor between December 2003 and April 2004, while he was looking for a professional job. PSR ¶ 100. Then, between May 3, 2004, and February 17, 2007, he worked at Morgan Stanley as a software engineer. PSR ¶ 98. Next, between February 2007 and April 13, 2008, he worked at Imagine Software "as a software engineer, writing codes for financial products and developing a real-time trading system for financial companies." PSR ¶ 97. The defendant was terminated from his employment after federal agents executed a search warrant at his office. PSR ¶ 97. One thing seems clear: His role in this conspiracy was plainly not his life.

E. Payments and Profits

Gonzalez was the clear and undisputed leader of the conspiracy. He made well over $1 million from the scheme. He paid substantial sums of money to Scott, Toey, and the others.

Again, however important the government contends Watt's role was in the TJX incursions, it has no evidence that he was ever paid for his efforts. In that regard, he stands alone.

II. GUIDELINE CALCULATION

The Guidelines calculation is:

Total Offense Level: 43

6 Base level for unlawful access to computers/access device fraud, § 2B1.1(a)(2)

+30 Loss over $400 million (here, $20 billion based on over 40 million credit cards stolen at $500 per card, Application Note 3(F)(i) to § 2B1.1), § 2B1.1(b)(1)(P)

+6 More than 250 victims, § 2B1.1(b)(2)(C)

+2 Use of sophisticated means, § 2B1.1(b)(9)(C)

+2 Trafficking of unauthorized access devices, § 2B1.1(b)(10)(B)(i)

+2 Use of special skill, § 3B1.3

–2 Minor role, § 3B1.2(b)(2)

–3 Acceptance of responsibility, § 3E1.1(a), (b)

Criminal History: 0 points, Category I

The defendant disputed (a) the amount of loss attributable to Watt, (b) the number of victims, (c) that his conduct involved the trafficking of unauthorized access devices or the use of special skills. He also contested the role adjustment, claiming that his was a "minimal" not a "minor" role. Accordingly, defendant recommended a sentence of probation or imprisonment of no more than six months.

The government recommended the maximum statutory sentence of 60 months. It should be noted that the Guidelines are almost irrelevant here, to the extent that they are completely

trumped by the maximum sentence. They call for a sentence of *life*, largely based on the amount stolen.[9]

I reject the defendant's Guideline challenges. The above recitation of the facts of this case demonstrates the legitimacy of the enhancements. I do believe, however, that a different sentence is called for under 18 U.S.C. § 3553(a) than the sentence apparently called for by the Guidelines, namely, the maximum sentence of 60 months.

A. Loss – USSC § 2B1.1

USSG §1B1.3(a)(1)(A) holds Watt accountable for all the acts he caused or abetted, while USSG § 1B1.3(a)(1)(B) holds him accountable for all acts and omissions of others that were in "furtherance of the jointly undertaken criminal activity" and "were reasonably foreseeable" to him. Watt pled guilt to a conspiracy from 2003 to 2008, the overt acts focusing on the "sniffer" program. The Guidelines hold him responsible for the totality of the loss, as an initial matter, before other adjustments. The loss here is pegged at the greater of "'actual loss,' defined as the 'reasonably foreseeable pecuniary harm that resulted from the offense,' and 'intended loss' as the pecuniary harm that was 'intended to result from the offense.'" United States v. Marti-Lon, 524 F. 3d 295, 301 (1st Cir.2008) (quoting U.S.S.G. § 2B1.1(b)(1) cmt. n.3(A)(i)-(ii)). Virtually any calculation of loss over $2.5 million would have led to a Guideline range at the statutory maximum. Even if Watt were only responsible for the TJX losses, the total loss attributable to TJX exceeds that figure.

[9] In this instance, I am reminded of a quote from United States v. Parris: "Although I began the sentencing proceeding 'by correctly calculating the applicable Guidelines range,' . . . it is difficult for a sentencing judge to place much stock in a guidelines range that does not provide realistic guidance." 573 F. Supp. 2d 744, 751 (E.D.N.Y. 2008).

The real question is the relationship to the loss figure to the issues raised in 18 U.S.C. § 3553(a). Loss under the Guidelines is effectively a proxy for evaluating culpability. Sometimes it is appropriate, and sometimes it is not. See United States v. Costello, 16 F. Supp. 2d 36 (D. Mass. 1998). For example, at one point, the background note to USSG § 2B1.1 suggested that the Guideline drafters believed loss was an appropriate proxy because it reflected both "harm to the victim" and "gain to the defendant."[10] As in the Costello case, that was not so here; Watt made nothing from the scheme. See Costello, 16 F. Supp. 2d at 38-39 (departure for a defendant whose "cut" of the scheme was less than 1% of the value of the goods stolen).

Other courts have described this issue more generally, not necessarily keyed to victim harm or defendant gain. The Third Circuit noted that loss can, for a peripheral defendant in a conspiracy "overstate both the degree of [defendant's] criminality and his need to be corrected." United States v. Stuart, 22 F. 3d 76, 82 (3d Cir. 1994); see also U.S. v. Emmenegger, 329 F. Supp. 2d 416, 427 (S.D.N.Y. 2004). Typically, this is so because the Guideline adjustments for role -- four points for minimal role, two points for minor role -- rarely compensate for the impact of a substantial loss.

The defendant insists that he "only" worked on the sniffer program, and thus should not be held responsible for the totality of the loss to TJX. (His sniffer program was "only" used for TJX.). The defense minimizes the contribution, describing the sniffer program Watt adapted as

---

[10] This comment stated:

> The value of the property stolen plays an important role in determining sentences for theft and other offenses involving stolen property because it is an indicator of both the harm to the victim and the gain to the defendant.

USSG § 2B1.1, cmt. background (U.S.S.G. app. C, amend. 617).

elementary, even available in the public domain. Watt does not deny that he added value to the scheme, using his special skills to edit the sniffer program. What he seems to be saying is that his contribution was not indispensable. In effect, he suggests, anyone could have done it. But not "anyone" did.

The government counters that Watt was far more culpable because he knew what Gonzalez and his co-conspirators were doing. Watt and Gonzalez were close friends, going back to their teenage years. (Indeed, most of the co-conspirators, like Scott and Gonzalez, were friends since high school.) Gonzalez had enlisted Watt's help before. They worked together in 2005 to exploit network vulnerabilities in Florida International University's network. PSR ¶ 16a.

Moreover, the government underscores the importance of the 300 instant message exchanges between Gonzalez and Watt from February 2005 until April 2006, which strongly suggest that Watt knew what was happening with his code. In one, dated March 8, 2005, Gonzales speaks in clear terms about his activity in hacking into computer systems, stealing payment card numbers, and selling them at a handsome profit. Gonzales bragged repeatedly to Watt about the scope of the fraudulent scheme, even sending him news articles about the damage he was inflicting. The government points to certain episodes that must have tipped Watt off to the scale of the crimes: Several times, Watt attended lavish parties thrown by Gonzalez, including a $75,000 birthday bash; another time, Gonzalez told Watt that he was having trouble counting $340,000 in $20 bills (the denomination in which ATMs dispense cash), because his mechanical money-counter was broken.

Still, Watt claims that he did not know about the specifics, did not access any of the information stolen, did not profit and that some of the back and forth with Gonzalez was just

bravado**.** These facts alone should give a sentencing decision-maker pause about the appropriateness of ascribing the full loss to Watt.

B. Role

To be sure, Watt is entitled to a minor role adjustment under USSG § 3B1.2(b). He was not as insignificant a participant as two of the defendants in Costello. Those defendants were fungible players in the warehouse theft, a man in the shipping department and a second in packaging; anyone could have assumed their role in the conspiracy and would have been paid as little. Watt's role was not fungible. Whether complex or not, his program played an important part in at least some of the incursions. But there is no dispute that Watt was less culpable than the leader, Gonzalez, and the others, like Scott and Toey, who were, as the government noted, "the ones who were on the ground trying to hack into the machines." Transcript of June 8, 2009, p. 11, and others whose role was to move money. Id. at 12-13.

As such, I concluded Watt had a "minor" role, but not a "minimal" one under the guidelines.[11]

III. 18 U.S.C 3. 3553(a)

A. Deterrence.

One of the purposes of sentencing under 18 U.S.C. § 3553(a) is deterrence, a purpose which has a particular resonance here. As one author describes, deterrence and punishment are particularly important for cybercrimes:

> [C]ybercrimes by their very nature allow offenders to commit the offenses without leaving their homes and with a veil of anonymity. This lack of contact with the victims of their crimes and insulation

[11] I also reject defendant's other Guideline challenges.

> from law enforcement may cause them to be under-deterred. Only successful prosecution and significant punishment will supply prospective cyber-criminals with the information needed to create real deterrence.

Richard Downing, Prosecution Responses to Internet Victimization: Thinking Through Sentences in Computer Hacking Cases: Did the U.S. Sentencing Commission Get It Right?, 76 Miss. L.J. 923, 925-26 (2007).

The need for deterrence -- general deterrence here -- plainly calls for punishment beyond probation or six months' imprisonment. 18 U.S.C. § 3553(a)(2)(B).

This is so especially given Watt's motives. Again, the government points to the emails which suggest that Watt was motivated by malicious intent to take down corporations and individuals rather than personal financial gain. Watt had said there was a "rush" about "ripping off somebody large and powerful." Exhibit 1(a). He also said, "[W]hat really drove me harder and further was the exciting possibility of using computers to turn the life of a particular fellow human being into a living hell." Exhibit 1(b) at 3. The challenge of finding vulnerabilities in computer systems made him "feel like a hacker from *The Matrix*." Id. at 4. And describing the feeling he gets from hacking: "It's distinguished by an acutely defined and unparalleled sense of schadenfreude" (pleasure from the misfortune of others). Id. at 3. Watt's counsel argued that these quotes mischaracterized Watt's motives, and were out of context. Some came from a website, "Phrack," known for including jokes and other sarcastic comments by hackers.

I have seen emails like this before, arguably a certain badinage that is made darker, more conspiratorial when played out on the internet. See supra n.7. Nevertheless, they are surely relevant. They suggest, at best, that Watt did not care about the damage he was causing.

Again, one can distinguish between types of computer crimes:

> In the case of damage to a computer, however, the actor could have a variety of mental states. In some cases, the offender has acted intentionally to access a computer without authorization but then inadvertently causes the system to crash. This negligent or reckless damage can have serious consequences – such as when a juvenile shut down the regional airport in Worcester, Massachusetts, in 1996 by breaking into a telephone company computer and accidentally causing the machine to crash – but the offender should be treated more leniently than if the conduct were fully intentional. By contrast, Jeffery Lee Parson released a worm that not only spread aggressively and monopolized communications bandwidth, but it caused computers around the world to deluge Microsoft with spurious data that shut down its Internet connection for hours. Plainly, courts should treat these two offenders differently due to their differing degrees of intent, quite apart from the damage that their acts actually cause.

Downing, supra, at 932-933.

Watt was somewhere in between the examples described above. He was playing with codes and software to help his friend and having fun doing it, all the while having a full time job. But he also knew on some level that he was wreaking havoc on people's lives. All this calls for punishment far more substantial than the defense seeks.

B. First Offender

Watt is a first offender, with no prior criminal activities. He once had a bright future and a promising career in computer-related fields within securities and financial services. He has been fired from his job at Imagine Software -- appropriately so**.** His chances of a career in this area are probably nil.

The Sentencing Reform Act, 28 U.S.C. § 994(j), directed the Sentencing Commission to "insure that the guidelines reflect the general appropriateness of imposing a sentence other than

imprisonment in cases in which the defendant is a first offender who has not been convicted of a crime of violence or an otherwise serious offense." Id.

As I noted in United States v. Germosen, 473 F. Supp. 2d 221, 227 (D. Mass. 2007), the Commission has not done so. It redefined "serious offense" in a way that was entirely inconsistent with prior practice, and not at all based on any real data or analysis. First offender status was folded into criminal history category I. Category I included those who had never had any encounters with the criminal justice system, never been arrested, as well as individuals who had been arrested and convicted but received short sentences. Shortly after the implementation of the Guidelines, it was clear that the Commission's decisions led to a far higher incarceration rate for non-violent first offenders than had been the pattern pre-Guidelines.

And that result plainly does not comport with deterrence. The Sentencing Commission's report, Recidivism and the "First Offender" (May 2004), available at http://www.ussc.gov/publicat/Recidivism_FirstOffender.pdf, suggests that individuals -- like Watt -- with zero criminal history points are less likely to recidivate than all other offenders. Commission studies show that the recidivism rate for such individuals is substantially lower than recidivism rates for other offenders, and even for offenders with only one criminal history point. Id. at 13.

For all of the above reasons, I concluded that based primarily on the factors set forth in 18 U.S.C. §§ 3553(a)(2)(A) (the need for a sentence "to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense") and (B) ("to afford adequate deterrence to criminal conduct") a meaningful period of incarceration was called for. As the Court noted in Emmenegger: "To permit such an offender to avoid meaningful incarceration,

while jailing thieves and other non-violent offenders of lower social status, would trivialize the seriousness of white-collar offenses." 329 F. Supp. 2d at 427. I conclude that a sentence of two years is a sentence that meets the parsimony principle embodied in the statute, a "sentence sufficient, but not greater than necessary, to comply with the purposes" of sentencing in 18 U.S.C. § 3553(a). Two years in a federal prison is a long time for someone who has never been to prison before. Moreover, whatever punishment is inflicted by this sentence will be exacerbated by the substantial restitution and the impact of this high profile felony conviction.

SO ORDERED.

Date: April 27, 2010

/s/ Nancy Gertner

NANCY GERTNER, U.S.D.C.

Publisher Information

Note* This page is not part of the opinion as entered by the court. The docket information provided on this page is for the benefit of publishers of these opinions.

1:08-cr-10318-NG USA v. Watt
Date filed: 10/29/2008
Date terminated: 03/23/2010
Date of last filing: 04/27/2010

Attorneys

Michael C. Farkas 381 Park Avenue South 16th Floor New York, NY 10016 212-760-8400 212-760-8403 (fax) mfarkas@farkaslawfirm.com Assigned: 03/06/2009 PRO HAC VICE ATTORNEY TO BE NOTICED	representing Stephen Watt (1) TERMINATED: 03/23/2010 (Defendant)
Robert M. Goldstein 20 Park Plaza, Suite 1000 Boston, MA 02116 617-742-9015 617-742-9016 (fax) rmg@goldstein-lawfirm.com Assigned: 12/15/2008 ATTORNEY TO BE NOTICED	representing Stephen Watt (1) TERMINATED: 03/23/2010 (Defendant)
Stephen P. Heymann United States Attorney's Office 1 Courthouse Way Suite 9200 Boston, MA 02210 617-748-3100 Stephen.Heymann@usdoj.gov Assigned: 10/29/2008 LEAD ATTORNEY ATTORNEY TO BE NOTICED	representing USA (Plaintiff)